

UNITED STATES DISTRICT COURT

for the
Western District of VirginiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
1850 River Inn Lane
Charlottesville, Virginia 22901

)

Case No. 3:22mj00036

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-1

located in the Western District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| <i>Code Section</i> | <i>Offense Description</i> |
|------------------------|---|
| 18 U.S.C. § 371 | Conspiracy to Defraud the United States; Make a False Statement or |
| 18 U.S.C. § 1001(a)(2) | Representation to a Department or Agency of the United States; and Wire Fraud |
| 18 U.S.C. § 1343 | |

The application is based on these facts:

See attached affidavit

Continued on the attached sheet.

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Clifford Paul Greene

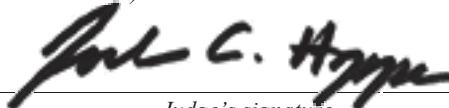
Applicant's signature

Clifford Paul Greene, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ (specify reliable electronic means).

Date: 8/10/22



Judge's signature

City and state: Charlottesville, Virginia

Joel C. Hoppe, United States Magistrate Judge

Printed name and title

ATTACHMENT A-1

TARGET RESIDENCE

The a single-family residence located at 1850 River Inn Lane, Charlottesville, Virginia 22901 (**TARGET RESIDENCE**), which is a three-story residence with a side-entry garage. The **TARGET RESIDENCE** includes the interior of the residence and garage, as well as any exterior areas such as the porch or exterior shed(s), and any vehicles parked in the driveway or within the garage. Below is an image of the front of the residence.



ATTACHMENT B-1

Information to be searched for and seized by Law Enforcement Personnel from the

TARGET RESIDENCE, as described in Attachment A-1:

All information that constitutes evidence and instrumentalities concerning violations of 18 U.S.C §§ 371 (Conspiracy), 1001(a)(2) (False statements to Government Agents or Agencies), , and 1343 (Wire Fraud) (collectively, the “Target Offenses”):

1. **RECORDS, DOCUMENTS, DATA AND INFORMATION:** Any records, documents, data, information, computer executable programs, email messages, correspondence, communications, and/or attachments that contain or related to the information described in the subsection below whether located in hard-copy or in electronic-format within any computer, cellphone, tablet device, or other electronic storage medium:

a. Applications, proposals, or contracts involving research grant funding, laboratory resources, research assistance, work-related travel funding, work-related reimbursements and/or employment involving: (1) Gang TAO (“TAO”) and any federal agency of the United States (including the National Science Foundation) or (2) TAO and the People’s Republic of China, the National Science Foundation of China, Nanjing Aeronautics and Astronautics University, and/or any other Chinese-based entities (collectively, “People’s Republic of China”);

b. Patents applications, patent awards, patent royalty payments, entity structures or other information related to the possession of intellectual property involving TAO, including, but not limited to those involving the following areas:

the probabilistic self-adapting compensation method of satellite attitude control system; a kind of fault tolerant control method and control system of drive lacking Rigid-body System; a kind of method for building up of model for the bullet train lengthwise movement containing interference; bullet train actuator adaptive failure compensates location tracking method; A kind of self-adapting compensation method of satellite attitude control system actuator hardover failure; a kind of Adaptive Compensation Control Method of non-minimum phase flight control system actuator sustained intermittent failure; train suspension system fault diagnosis and fault-tolerant control method based on dynamic actuator; fault-tolerant control method and system of under-actuated rigid body system; and self-adaptation compensation method for uncertainty of drive signs of actuator of satellite attitude control system;

c. Employment contract stipulations, proposals, or provisions involving **TAO** and the People's Republic of China, Thousand Talent Plan and/or ChangJiang Scholar Program;

d. Any payment, movement, or transfer of funds to/from or at the direction of **TAO** or **Lanlin Chen (CHEN)** via Alipay and Huaxia Bank or any other Chinese-based banking institution or application;

e. Information, records, or assets involving bank accounts under the control of **TAO** and/or **Chen**, assets exceeding a value of \$1,000, or the receipt of bulk cash;

f. **TAO**'s travel to or from the People's Republic of China, including reservation records, passports, and/or photographs of travel;

- g. Any presentations, lectures, research, or publications related to the People's Republic of China;
- h. Any information involving the following individuals and/or email addresses: Ruiyun Qi; ruiyun.qi@nuaa.edu.cn; Bin Jiang; binjiang@nuaa.edu.cn; Xing Yu; Gong Huajun; ghj301@nuaa.edu.cn; Yang Hao; haoyang@nuaa.edu.cn; Tan Chang; lovetanchang@163.com; Yang Hao; haoyang@nuaa.edu.cn; Wen LiYan; wenliyan8710@163.com; and any email address ending in @nuaa.edu.cn or ending in @163.com.
- i. Research conducted on behalf of/in connection with the People's Republic of China;
- j. Any records involving the receiving or sending of shipments, packages, or other items to/from China;
- k. **TAO**'s employment status, income, or expenses;
- l. Information regarding any student(s) attending Nanjing Aeronautics and Astronautics University or seeking sponsorship to serve as an international student from China and studying at the University of Virginia;
- m. Any logs, passwords, or other documentation showing access to or communications involving financial accounts/applications;
- n. Any logs, passwords, or other records involving the use of WeChat by **TAO** to communicate with Ruiyun Qi; Bin Jiang; Xing Yu; Gong Huajun; Yang Hao; Tan Chang; Yang Hao; Wen LiYan; or any identified student, employee or affiliate of Nanjing Aeronautics and Astronautics University;

- o. Research articles or journal publications written by **TAO** wherein he describes research, findings, and/or funding resources;
- p. Any other evidence indicating the state of mind or intent of **TAO** as it relates to the Target Offenses, including contextual information necessary to understand the evidence described in this attachment, which constitutes evidence of the Target Offenses; and
- q. The identities of individuals with access to the above-listed categories of information involving **TAO**;

2. **COMPUTER RELATED SEIZURES:** For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant:

- a. Evidence of who used, owned, or controlled the computer or storage medium at the time the things described in this warrant were created, edited, or deleted, such as logs, IP addresses, routing information, methods of connection, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control or track the computer or storage medium, such as viruses, cookies, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;

- d. Evidence indicating how and when the computer or storage medium was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. Evidence computer user's state of mind as it relates to the crime under investigation; evidence of the attachment to the computer or storage medium of other storage devices or similar containers for electronic evidence;
- f. Evidence of counter-forensic programs (and associate data) that are designed to eliminate data from the computer or storage medium;
- g. Evidence of the times the computer or storage medium was used;
- h. Passwords, encryption keys, and other access devices that may be necessary to access the computer or storage medium;
- i. Documentation and manuals that may be necessary to access the computer or storage medium or to conduct a forensic examination of the computer or storage medium;
- j. Records of or information about Internet Protocol addresses used by the computer or storage medium;
- k. Records of or information about the computer or storage medium's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- l. Contextual information necessary to understand the evidence described in this attachment.

3. OTHER PHYSICAL EVIDENCE:

- a. Any bulk cash, cashiers' checks, or other foreign currency with a value exceeding a U.S. currency value of \$1,000; and
- b. Passports.

4. DEFINITIONS

- a. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
- b. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- c. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, flash memory, CD-ROMs, and other magnetic or optical media.
- d. As used above, the terms "records," "documents," "data" and "information" include all of the forgoing items of evidence in whatever form and by whatever means they may have been created or stored.

5. REVIEW OF ELECTRONIC MEDIA: This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.